ABSTRACT

A method for detecting surveillance activity in a computer communication network comprising automatic detection of malicious probes and scans and adaptive learning. Automatic scan / probe detection in turn comprises modeling network connections, detecting connections that are likely probes originating from malicious sources, and detecting scanning activity by grouping source addresses that are logically close to one another and by recognizing certain combinations of probes. The method is implemented in a scan/probe detector, preferably in combination with a commercial or open-source intrusion detection system and an anomaly detector. Once generated, the model monitors online activity to detect malicious behavior without any requirement for a priori knowledge of system behavior. This is referred to as "behavior-based" or "mining-based detection." The three main components may be used separately or in combination with each other. The alerts produced by each may be presented to an analyst, used for generating reports (such as trend analysis), or correlated with alerts from other detectors. Through correlation, the invention prioritizes alerts, reduces the number of alerts presented to an analyst, and determines the most important alerts.